REMARKS

Claims 1-20 were pending. Claims 1, 3-7, 9-13, 15 and 17-20 have been amended. Claims 2 and 16 have been cancelled. Claims 21-23 are newly submitted. No new matter has been added. Accordingly, claims 1, 3-15 and 17-23 remain pending in the application. Reconsideration is respectfully requested in view of the amendments to the claims and the following remarks.

I. The § 112 Rejections

Claims 6 and 13 were rejected under 35 U.S.C. § 112, first paragraph, as being based on disclosure which is not enabling. Applicant respectfully disagrees.

Claim 6 recites validating and decrypting the trusted messages in the managed client systems to perform the service commands. Claim 13 recites the at least one client system validates and decrypts the trusted messages to perform the service commands. The Examiner asserts that in order to decrypt a message, the message must first be encrypted. While Applicant does not disagree with the Examiner's assertion, Applicant submits that one of ordinary skill in the art would readily recognize Applicant's claimed "*trusted* messages" represent encrypted communications. As disclosed in the specification, "the data center 18 issues an appropriately signed, trusted message to the intended client 16, 16a, 16b or 16c" (page 4, lines 20-21). "The client system 16, 16a, 16b or 16c then validates the signature of the received message and decrypts the message" (page 5, lines 2-3). Because the messages sent from the data center to the client system are *trusted* messages, the client system, therefore, needs to perform steps of "validating and decrypting the trusted messages". Thus, claims 6 and 13 are not indefinite under 35 U.S.C. §112, first paragraph.

II. The § 102/103 Rejections

Claims 1-4, 7, 9-11 and 14-18 were rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 6,157,953 ("Chang").

Claims 5-6, 12-13 and 19-20 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Chang in view of U.S. Patent No. 6,665,674 ("Buchanan").

Applicant respectfully traverses.

A. Independent Claim 1

Claim 1 recites verifying authentication of an administrator system by a data center. The administrator system is a computer through which an administrator manages at least one of a plurality of client systems.

A potential advantage of verifying authentication of the administrative system (or computer) is that such authentication prevents the opportunity for unauthorized administrative use when the computer system is not present (specification page 5, lines 14-16).

Chang discloses a system for the administration of services residing on multiple service host computers from an administration server computer (see Abstract). In particular, Chang's system operates as follows. A user identifier (or user name) and a corresponding password are provided to a service manager. The service manager authenticates the user by comparing the user identifier and password against a list of user identifiers and corresponding passwords stored in a persistent memory.

While Chang discloses verifying user identifiers (and corresponding passwords), Chang clearly does not disclose verifying authentication of an administrator system (or computer).

Claims 3-6 depend from claim 1, and are allowable over Chang for at least those reasons that apply to claim 1.

Claims 15 and 23 (and the claims that depend therefrom) include limitations similar to claim 1, and are also allowable over Chang for at least those reasons that apply to claim 1.

B. Independent Claim 7

Claim 7 recites a data center that receives a service command from an administrator system, and issues a trusted message to remotely control a client system. The data center receives the service command after authentication of a first user associated with the administrator system, and the data center issues a trusted message to the client system after authentication of a second user associated with the data center. The first user is different from the second user.

Chang fails to disclose a system that authenticates two different users while managing a client system – i.e., a first user associated with an administrator system, and a second user associated with a data center. Instead, Chang discloses a system that includes a *single* user sign on for authentication relating to management of services on service hosts from a browser host (col. 12, ll. 20-22). Within Chang's system, information is handled and transmitted to each service host that a system administrator wants to manage without having the administrator re-authenticate on each individual service host (col. 12, ll. 28-31). Thus, in Chang's system only a single user is authenticated during management of a service host.

Claims 8-14 depend from claim 7, and are allowable over Chang for at least those reasons that apply to claim 7.

In view of the foregoing, it is submitted that the claims 1, 3-15 and 17-23 are allowable over the cited references, and are in condition for allowance. Should any unresolved issues remain, the Examiner is invited to call Applicant's attorney at the telephone number indicated below.

Respectfully submitted,
SAWYER LAW GROUP LLP

July 7, 2005

Kelvin M. Vivian
Attorney for Applicant(s)
Reg. No. 53,727
(650) 493-4540